Date of Hearing: June 19, 2007

ASSEMBLY COMMITTEE ON JUDICIARY
Dave Jones, Chair
SB 30 (Simitian) – As Amended: June 12, 2007

SENATE VOTE: 33-3

SUBJECT: IDENTIFY INFORMATION PROTECTION ACT OF 2007

KEY ISSUES:

1) SHOULD THE LEGISLATURE ENACT INTERIM MEASURES TO ADDRESS THE PRIVACY AND SECURITY ISSUES RAISED BY THE INCREASING USE OF SO-CALLED "RFID" DEVICES IN GOVERNMENT-ISSUED IDENTIFICATION CARDS?

2) SHOULD THE CALIFORNIA RESEARCH BUREAU CONDUCT A STUDY RELATING TO RFID PRIVACY AND SECURITY ISSUES, FOR THE PURPOSE OF PROVIDING INFORMATION THAT WILL GUIDE THE LEGISLATURE IN ENACTING PERMANENT MEASURES TO REPLACE THE INTERIM MEASURES CREATED BY THIS BILL?

SYNOPSIS

This bill is one of several by this author that seek to regulate the use of radio frequency identification devices (RFID) and other technologies that permit the remote reading of data stored on government-issued identification cards. This bill is quite similar to last year's SB 768, by the same author, insofar as it calls for interim security measures for government-issued RFID devices until such time as the Legislature enacts permanent measures based on a required study and report to be provided by the California Research Bureau. However, last year's bill also included criminal provisions making it unlawful for a person to "skim" or attempt to obtain information from an RFID card without the cardholder's knowledge or consent. This criminal provision has been removed from SB 30 and now exists as a stand alone bill SB 31, which will not likely be heard by this Committee. Last year's SB 768 was the result of extensive deliberations between the author, various privacy and consumer groups, and representatives from the technology industry, including businesses that develop, manufacture, or sell remote reading technology. Although the two sides apparently reached an accord of some sort and SB 768 passed both houses of the Legislature, it was vetoed by the Governor. It is not clear how, if at all, this year's SB 30 will address the Governor's concerns. The author and supporters contend that this bill is necessary to protect Californians from the serious privacy and security risks associated with RFID technology, especially in light of the fact that RFID devices can transmit personal information without the knowledge or consent of the device holder. Opponents contend that the bill is unnecessary, that there have been no real life cases linking RFID to identity theft, and that the author and supporters misrepresent the capabilities (and therefore the alleged risks) of RFID technology. In addition, the opponents claim that some of the specific provisions of this bill may unintentionally undermine safety and security. The interim measures proposed by this bill would sunset in 2012. In the meantime, the bill calls upon the California Research Bureau to conduct a study on RFID privacy and security issues and make a report to the Legislature no later than June 30, 2008. It is the intent of this bill that the Legislature will

then enact permanent security measures based in part on that report in as timely a manner as possible.

SUMMARY: Enacts the Identity Information Protection Act of 2007 to (1) establish interim privacy and security protections to apply to remotely readable identifications (IDs) created, mandated, purchased, or issued by government entities, until subsequent legislation or regulations are enacted, (2) require the California Research Bureau to submit a report to the Legislature on security and privacy for government-issued, remotely readable IDs on or before June 30, 2008, and (3) specify that it is the intent of the Legislature that the interim measures contained in the Act be replaced with permanent legislation or regulations in the most timely and expeditious fashion possible following the issuance of the California Research Bureau's report. Specifically, this bill:

1) Requires, generally, that a government entity that issues identification documents (IDs) that use radio waves to transmit data or enable data to be read remotely must implement certain security measures, depending for the most part upon the nature of information that is stored on, or transmitted by, the ID. Provides that ALL such IDs must at minimum incorporate tamper-resistant features and implement an authentication process.

2) Provides that if personal information, as defined, is transmitted remotely from the ID, the issuing entity must ensure all of the additional security features: (a) the ID and authorized readers must use a "mutual authentication process;" (b) the ID must make the information unreadable and unusable by an unauthorized reader through means of encryption or some other means that renders the information indecipherable; (c) the ID must implement an access control protocol that enables the holder to exercise direct control over the transmission of the data, not including a detachable shield device.

3) Provides that if a unique personal identifier is used to provide an individual with more than one type of application or service, then the issuing entity shall do one or more of the following, commensurate with the sensitivity of the application: (a) implement a secondary verification and identification procedure that does not use radio waves, including manual entry of a number on a keypad; (b) implement a mutual authentication process; (c) use encryption or some related security measure that makes the information unreadable and unusable; (d) implement an access control protocol that gives the holder direct control over the information, not including a detachable shield device. Specifies further one or more of these requirements must be met for certain remotely readable IDs issued by public schools, for purposes of accessing transit services, or issued to members of the public pursuant to Section 6552 of the Government Code, as specified.

4) Requires the issuing entity to make specified disclosures about the nature of the capability of the ID and its content, about countermeasures that the holder can take to control the transmission of information on the ID, and the location of authorized readers of the IDs.

5) Exempts from the security and disclosures requirements of this bill certain uses of remotely readable IDs, including systems implemented prior to January 1, 2008, or for which there is a contract or publicly issued proposal prior to September 30, 2007. Further exempts IDs issued in jails, prisons, or other detention facilities; IDs issued to law enforcement or emergency response personnel, subject to certain conditions; ID issued to specified persons or patients in certain institutions, including government-owned or operated medical facilities, if certain

conditions are met; IDs issued for patients or personnel in various medical emergency contexts; and IDs that are issued for the limited purpose of accessing a secured public building or parking structure, so long as certain disclosure requirements are met.

6) Provides that government entities that issue remotely readable IDs in compliance with this bill shall not disclose operational key systems to other entities or third parties and shall take reasonable measures to keep operational key systems secure.

7) Provides that a government entity that issues a remotely readable ID in compliance with this bill shall not disclose information regarding the location of a person, derived from the use of radio waves, unless the disclosure is made pursuant to an exigent circumstance, and certain verification steps are taken, or the disclosure is required pursuant to a search warrant.

8) Provides that, where a government entity violates the provisions of this bill, an interested person may institute proceedings for injunctive or declaratory relief or other performance writ, but only after providing prior written notice of the violation and allowing 30 days for the entity to cure the violation. Further provides that a party bringing an action may be entitled to fees and costs, and also specifies that this provision does not preclude other legal remedies available in law or equity.

9) Requires the California Research Bureau to assemble an advisory committee and submit a report to the Legislature, no later than June 30, 2008, related to security and privacy issues related to the use of remotely readable government IDs.

EXISTING LAW:

1) Provides that all people in this state have an inalienable, constitutional right to privacy. (Cal. Const., Art I, Sec. 1.) Protects people against significant intrusions upon their fundamental privacy and autonomy interests, except where the intrusion is "necessary to further a 'compelling'--i.e., an extremely important and vital--state interest," and where a feasible and effective alternative does not exist that would have a lesser impact on privacy interests. (Acad. of Pediatrics v. Lungren, (1997) 16 Cal. 4th 307, 330, 341.)

2) Precludes a state agency, under the Information Practices Act, from disclosing personal information it possesses "in a manner that would link the information disclosed to the individual to whom it pertains," except in specified circumstances. (Civ. Code Section 1798.24.) An agency is subject to a civil suit if it does not comply with these standards and a person suffers an adverse effect. (Civ. Code Section 1798.45.)

FISCAL EFFECT: As currently in print this bill is keyed fiscal

COMMENTS: This bill is one of several by this author that seek to regulate the use of radio frequency identification devices (RFID) and other technologies that permit the remote reading of data stored on government-issued identification cards. This bill is quite similar to the author's SB 768, of last year, insofar as it calls for interim security measures for government-issued RFID devices until such time as the Legislature enacts permanent measures based on a required study and report to be provided by the California Research Bureau. In general the bill does three things: (1) establishes interim privacy and security protections to apply to remotely readable identifications (IDs) created, mandated, purchased, or issued by government entities, until

subsequent legislation or regulations are enacted, (2) requires the California Research Bureau to submit a report to the Legislature on security and privacy for government-issued, remotely readable IDs on or before June 30, 2008, and (3) specifies that it is the intent of the Legislature that the interim measures contained in this bill be replaced with permanent measures in the most timely and expeditious fashion possible following the issuance of the California Research Bureau's report.

The specific security provisions, which are detailed above, essentially create three different levels of security protection depending upon the kind of information that is contained on the card and, to a lesser extent, depending on how the card will be used. First, all cards, including those without "personal information," will be required, at the very least, to use some tamper resistant feature to prevent duplication, forgery, or cloning, and to employ some form of authentication, which ensures that the reader is permitted to read the information on the ID. Second, for documents that contain "personal information" (which is defined to include name, address, social security number, etc.), the card must employ additional higher standards, including encryption, access control protocols, and "mutual authentication" (a means by which card and reader can essentially verify each other). Third, for cards that contain only a "unique personal identifier" (a randomly assigned string of numbers that, despite the name, identifies the document, not the individual) but is used for more than one purpose (e.g. a university student ID card used at the library and the cafeteria) must implement a system of secondary verification (such as manual entry into a keypad) or employ one or more of the measures required for the other two categories.

Background: What is RFID and How Does it Work? Despite the jargon-laden language sometimes used by both proponents and opponents, the basic outline of how RFID and related technologies works is fairly easy to understand. RFID "tags" can be embedded into objects, including documents, clothing, and even people. The tag typically consists of a microchip (that stores information) and one or more antennae. Remote “readers” can read this tag, via radio waves. The reader constantly emits radio signals. As a person or object with an RFID tag moves near the reader – the distance varies depending upon the device – the antennae pick up the signal and transmit the information stored on the microchip to the reader. Most RFID tags are "passive," which means that they can only be activated by the radio signal; others are "active," which means that they can actively search out readers in the area. In either case, an authorized reader can then transmit this information to a computer database. The distinction between "passive" and "active" tags is important because, despite some claims to the contrary, a passive tag cannot "broadcast" any information, personal or otherwise.

In some ways, RFID technology is merely a higher-tech version of bar code and magnetic strip scanning. However, scanning requires direct contact between the scanner and the stored information (or at least the magnetic strip or barcode must be in the direct line of sight of a laser). RFID readers, on the other hand, can read the information stored on the RFID tag remotely. With existing technology, the reader's capacity may only be about an inch or several feet. Experts disagree on the *potential* range of RFID readers in the future. But most agree that the current technology typically only works at ranges of a few inches, though some devices may have ranges up to thirty feet. However, the fact that RFID tags can be read at any distance creates the possibility that information stored on an identification document can be read without the holder's knowledge or consent.

A key issue that divides experts on both sides of the debate, however, concerns the nature of the information stored on the RFID tag, and the usefulness of that information to any unauthorized reader. Sometimes an RFID tag only contains a random number that has no meaning until the reader transmits it to a computer database, where the random number is then matched to other information. However, RFID tags apparently can contain other information, such as a name, address, a credit card number, or even a visual image. Experts on both sides of the debate disagree about the value of "encryption" or other security measures that make stored information intelligible only to authorized readers. Moreover, privacy advocates point out that security measures must address more than the ability of the reader to access intelligible information from the tag; they must also address potential security breaches along the entire transmission process from tag, to reader, to computer database. Proponents of RFID, on the other hand, claim that RFID applications are confined to a closed system of authorized tags, readers, and databases within that system. So that even if outsiders with remote readers obtained information from an RFID tag, that information is only intelligible to persons within the system. (The above summary of RFID technology, and the contours of the debate of privacy and security issues, is based, in part, on a host of documents representing the opinions of privacy rights and consumer groups, industry representatives, and government agencies. See for example www.privacyrights.org/are/RFIDposition.htm.)

ARGUMENTS IN SUPPORT: According to the author, this bill is needed because "RFID-enabled IDs can be, and have been, easily compromised." In support of this contention, the author cites various news reports and three federal studies – one by the Department of Homeland Security (DHS) and two by the Governmental Accountability Office (GAO). These studies raised questions about both the *effectiveness* of RFID for purposes of human identification and the *privacy and security* implications of the widespread use of RFID. A 2005 study conducted by the Governmental Accountability Office (GAO), as the author summarizes it, "found multiple problems with the technology, including significant privacy and security implications, as well as numerous operational issues (false readings, unreadable tags) and potentially harmful environmental impact (e-waste)." (See Department of Homeland Security, Data Privacy and Integrity Advisory Committee, *The Use of RFID for Human Identity Verification*, Report No. 2006-02, December 6, 2006; and GAO Study 05-551, May 2005; and GAO Study 07-248, December 2006.)

The author claims that "Government isn't alone in questioning security of RFID" and that "key actors in the technology sector recognize the privacy challenge RFID presents." In support of this bill and the others before this Committee, the author has submitted other reports, news stories, and anecdotal accounts that are supposed to demonstrate the risks and dangers of RFID technology. According to the author, RFID is an especially egregious form of identification document because it "broadcasts personal information" without the knowledge or consent of the cardholder. As noted below by the opponents, not all RFID have the capacity to "broadcast" information (most are passive) and most only transmit "personal information" if you include the random string of numbers that, according to the definitional section of this bill, only identify the identification document, not the individual card holder. Nonetheless the author and supporters contend that RFID, like most technologies, is ever evolving and expanding its capabilities. As would-be identity thieves hone their ability to construct make-shift "readers," any information "skimmed" from an RFID chip could potentially facilitate identity theft or work invasion of privacy.

The author points out that, despite these risks, there is no existing law that regulates the use of RFID technology or the kinds of information that can be placed on an RFID-enabled identification device. This bill, according to the author, will fill that statutory void – both in the short term by creating interim measures and, in the long term, by creating permanent standards based on the CRB study, if appropriate.

According to the ACLU, "data and identity theft are already rampant and the problems are getting worse." The uncontrolled and unregulated use of RFID technology, the ACLU believes, will only make this problem worse still. The ACLU, citing the 2005 GAO report (see above) claims that some of the key privacy issues raised by RFID include the need to notify individuals of the use or existence of the technology; the problem of tracking human movements and profiling individual habits; and the possible secondary uses of data skimmed from an RFID device. ACLU, therefore, supports this bill because it will create necessary interim measures that will protect the privacy and safety of Californians. A number of privacy rights groups and consumer groups support this bill for the essentially the same reasons as the ACLU, pointing again to the same GAO and DHS reports and suggesting at least the *potential* for abuse.

ARGUMENTS IN OPPOSITION: This bill is opposed by a number of retail, banking, and business associations, as well as various companies that manufacture RFID and related technologies. Their opposition to this particular bill must be placed in the context of their opposition to the several pending bills attempting to prohibit, limit, or regulate the use of RFID technologies. To all of these bills, they raise at least three core objections. First, opponents contend that these bills are largely unnecessary because, to date, there is no evidence that RFID technology has been linked to any particular case of identity theft. They claim that the supporters of this bill point to the same few reports, and the few instances that they point to are not real life examples, but staged, unrealistic, controlled experiments. Second, opponents claim that authors and proponents of these bills misrepresent the capabilities of RFID and thereby exaggerate the risks associated with its use. For example, they point to the fact that the authors and proponents routinely claim that RFID technology "broadcasts personal information," even though most RFID technologies contain only "passive" chips that do not "broadcast" anything and can only be activated by a reader. Moreover, they point out that the vast majority of RFID devices contain only a random number, not "personal information" as usually defined. Furthermore, because the range of most RFID readers is limited to a few inches, RFID is virtually useless for "tracking" human beings. Third, opponents stress that "not all 'RFID' is the same." There are vast differences – and vastly different security implications – between "passive" cards and "active" cards, between "smart cards" and "proximity cards," and between cards that truly contain "personal information" and those that contain only a random number. Most importantly, they argue, there is a vast difference between what can done with existing technology and what proponents claim might *conceivably* could be done in the future.

Beyond these general arguments, the opponents raise a number of more specific objections to this bill:

Potential Security Threats: Opponents claim that far from protecting our security, some of the specific provisions of this bill may actually jeopardize security. By requiring government entities to disclose the location of all readers (proposed Section 1798.10(a)(9)), this bill, the opponents claim, will provide helpful information to criminals and terrorists, since disclosing locations with readers is also disclosing locations without readers, and hence without access security.

"Exigent Circumstances" Requirements Excessive: Opponents also suggest that the "exigent circumstances" exemption is too burdensome. That is, proposed Section 1798.12(a) provides that a government entity shall not disclose any data or information regarding the location of a person using RFID technology unless there are exigent circumstances or disclosure is required by a search warrant. However, the bill qualifies the "exigent circumstances" exception by requiring that the issuing agency to first obtain from the person requesting the information (most likely an emergency medical responder) assurances that there is an immediate danger of death or serious bodily harm. The agency must also request various pieces of information, including the requester's name and title, the location and phone number of the office from which he or she works, and the name of that person's supervisor who has "ultimate operational responsibility" (a term that is not defined). After obtaining this information, the issuing entity then must contact the requester's supervisor in order to verify that the exigent circumstance exists. Opponents claim that this is an unrealistic requirement if a human life were truly in immediate threat of death or serious bodily injury.

RELATED PENDING LEGISLATION: SB 28 (Simitian): Prohibits, until January 1, 2011, the Department of Motor Vehicles (DMV) from issuing, renewing, duplicating, or replacing a driver's license or identification card, if the license or card uses radio waves to either transmit personal information remotely or to enable personal information to be read from the license or card remotely.

SB 29 (Simitian): Prohibits, until January 1, 2011, a public school, school district, and county office of education from issuing any device that uses radio waves to transmit personal information, as defined, or to enable personal information to be viewed remotely for the purposes of recording the attendance of a pupil at school, establishing or tracking the location of a pupil on school grounds, or both.

SB 362 (Simitian): Provides that no person shall require, coerce, or compel another person to undergo a subcutaneous implantation of identification device that transmits personal information, and provides for corresponding penalties and causes of actions.

SB 388 (Corbett): Requires any private entity that sells, furnishes, or otherwise issues a card or other item containing a radio frequency identification tag to make certain disclosures to the recipient cardholder.

REGISTERED SUPPORT / OPPOSITION:

Support

ACLU (co-sponsor)
Electronic Frontier Foundation (co-sponsor)
Privacy Rights Clearing House (co-sponsor)
ACLU of San Diego
AARP
Asian Americans for Civil Rights and Equality
California Commission on the Status of Women
California Federation of Teachers
Consumer Federation of America

California Immigrant Policy Center
California Labor Federation
Consumer Action
Consumer Federation of California
Consumers Union
Eagle Forum of California
Electronic Frontier Foundation
Gun Owners of California
Howard Jarvis Taxpayers Association
National Council of La Raza
Privacy Activism
Privacy Rights Clearinghouse
Protection and Advocacy, Inc. (PAI)
State Building and Construction Trades Council

Opposition

HID Global
Hi-Tech Trust Coalition:
- 3M
- AeA (American Electronics Association)
- ActivIdentity
- AIM Global
- Alvaka Networks
- Aubrey Group, Inc.
- American Express
- California Bankers Association
- California Business Properties Association
- California Chamber of Commerce
- California Financial Services Association California Retailers Association
- EDS
- Elpac Electronics, Inc.
- Grocery Manufacturers Association
- InCom Corp.
- Infineon Technologies North America Corp.
- Information Technology Association of America (ITAA)
- MAXIMUS
- Motorola
- Matheson Tri-Gas
- National Semiconductor
- Natoma Technologies, Inc.
- NXP
- Oberthur Card Systems
- Oracle Corporation
- Precision Dynamics
- Retail Industry Leaders Association
- San Jose Silicon Valley Chamber of Commerce
- SAS

Secura Key
SIA (Semiconductor Industry Association)
Sonnet Technologies, Inc.
Texas Instruments
VEDC, Inc.
Zebra Technologies

Analysis Prepared by: Thomas Clark / JUD. / (916) 319-2334